

سورین؛ راهکارهای پیشرفته امنیت سایبری

Advanced Cybersecurity Solutions

چرا سورین؟

مهندسی پیشرفته، محصولات نوآورانه و راهکارهای تخصصی امنیت سایبری

سورین با اتکا به دانش فنی تخصصی، توانمندی‌های مهندسی و رویکردی مبتنی بر نوآوری، در طراحی و توسعه محصولات پیشرفته و اجرای پروژه‌های پیچیده در حوزه امنیت سایبری فعالیت می‌کند. در سورین، تخصص و نوآوری در خدمت خلق فناوری‌های پیشرفته و ارائه راهکارهایی متمایز برای چالش‌های پیچیده سازمان‌ها قرار می‌گیرند.

شرکت دانش بنیان سورین، با هدف ارائه خدمات بصره، کارآمد و آگاهانه در حوزه دفاع سایبری در سال ۱۳۹۶ تاسیس شد و آغاز به کار کرد. سورین طیف وسیعی از خدمات امنیتی، نظیر مرکز عملیات امنیت (SOC)، امن‌سازی و مقاوم‌سازی (Hardening)، پاسخگویی و مدیریت حوادث امنیتی (CSIRT)، شکار تهدیدات سایبری، آموزش و آگاهی‌رسانی امنیتی (Security Awareness) را پوشش می‌دهد.



سورین یک مسیر شفاف و استاندارد برای ارائه بهترین نتایج به سازمان شما دارد.

• نیازسنجی

بررسی دقیق نیازها و چالش‌های سازمان

• ارزیابی

آسیب‌پذیری‌ها و تحلیل ریسک‌ها

• پایش و بهبود

پایش مستمر و بهینه‌سازی مداوم

• طراحی راهکار

طراحی راهکارهای مناسب با نیاز سازمان‌ها

• پیاده‌سازی

اجرای استاندارد‌ها و پی‌کربندی راهکارها

• پشتیبانی

پشتیبانی و همراهی بلند مدت



مرکز عملیات امنیت



پاسخگویی و مدیریت
حوادث امنیتی



شکار تهدیدات سایبری



امن‌سازی و مقاوم‌سازی



آموزش و آگاهی‌رسانی
امنیتی

امن سازی و مقاوم سازی (Hardening)

- طراحی معماری امنیتی شبکه مطابق با استراتژی مطرح
- استقرار راهکارهای امنیتی نظیر WAF، UTM، ...
- امن سازی و مقاوم سازی نرم افزار / سرویس های ویندوزی و لینوکسی
- امن سازی و مقاوم سازی پایگاه داده
- پیکربندی تجهیزات امنیتی شبکه

خدمات **Hardening** سورین با حذف تنظیمات ناامن، غیرفعال سازی سرویس های غیرضروری و پیاده سازی سیاست های امنیتی، سطح امنیت سامانه های سازمان را ارتقا داده و احتمال نفوذ و سوءاستفاده از آسیب پذیری ها را به حداقل می رساند.

شکار تهدیدات سایبری (Threat Hunting)

- شناسایی فعالانه تهدیدات پنهان، رفتارهای مشکوک و فعالیت های غیرعادی در زیرساخت های فناوری اطلاعات
- پیش از تبدیل شدن به رخدادهای امنیتی
- شکار تهدیدات دوره ای سیستم های ویندوز و لینوکس
- شکار تهدیدات دوره ای تجهیزات شبکه ای امنیتی
- گزارش تهدیدات احتمالی شناسایی شده
- گزارش نواقص پیکربندی (Misconfiguration) احتمالی در شبکه

خدمات و راهکارهای امنیت شبکه و زیرساخت



طراحی، پیاده سازی و ارزیابی مرکز عملیات امنیت

- استقرار راهکارهای مطرح مانیتورینگ امنیتی (Splunk، ELK، Wazuh و...)
- طراحی و تامین یوزکیس های (USECASE) اختصاصی و سفارشی
- طراحی و پیاده سازی بهینه و کارآمد مرکز عملیات امنیت
- ارزیابی بلوغ مرکز عملیات امنیت مطابق با استانداردهای مطرح
- طراحی و جاری سازی فرآیندهای مرکز عملیات امنیت
- تامین نیروی انسانی متخصص مرکز عملیات امنیت
- تامین لایسنس / ماژول های نرم افزاری مورد نیاز مرکز عملیات امنیت
- استقرار سنسورهای مطرح و کارآمد در مرکز عملیات امنیت (Sysmon، Zeek، Flow Generator و...)
- استقرار راهکارهای مکمل و افزوده مرکز عملیات امنیت نظیر Threat Intelligence، SOAR، Ticketing

در خدمات **Threat Hunting** سورین، کارشناسان امنیت با بررسی مداوم زیرساخت، تحلیل رفتار شبکه و شناسایی ناهنجاری ها، تهدیداتی را که ممکن است از سامانه های امنیتی عبور کرده باشند، کشف و کنترل می کنند تا ریسک های امنیتی سازمان به حداقل برسد.

01

Ai-powered SOC

سامانه‌ای هوشمند مبتنی بر هوش مصنوعی و عامل‌های هوشمند که با خودکارسازی تحلیل هشدارها، جمع‌آوری شواهد و همبستگی رخدادهای امنیتی، به تیم‌های SOC در شناسایی تهدیدها و تصمیم‌گیری سریع‌تر و دقیق‌تر کمک می‌کند.

محصولات امنیتی سورین

راهکارهای سورین با تمرکز بر کشف، تحلیل و مدیریت دارایی‌های سازمانی، دیدی جامع برای افزایش امنیت، کنترل و آگاهی عملیاتی فراهم می‌کنند.

02

Asset Intelligence

محصول Asset Intelligence (مدیریت هوشمند دارایی‌ها) یک راهکار جامع برای نظارت، دسته‌بندی و مدیریت دارایی‌های فناوری اطلاعات در سازمان‌هاست که با استفاده از فناوری‌های پیشرفته، به افزایش امنیت و بهره‌وری کمک می‌کند.



03

Threat Intelligence

محصول Threat Intelligence ابزاری پیشرفته برای جمع‌آوری، تحلیل و اشتراک‌گذاری اطلاعات تهدیدات سایبری است که با تحلیل داده‌های گسترده و به‌روز، به سازمان‌ها در پیش‌بینی، شناسایی و مقابله مؤثر با تهدیدات کمک می‌کند.

سورین با تکیه بر دانش بومی و تجربه تخصصی در حوزه امنیت سایبری، طراحی و پیاده‌سازی محصولات امنیتی نوآورانه را در دستور کار خود قرار داده است. این محصولات با هدف حفاظت از زیرساخت‌های حیاتی، افزایش تاب‌آوری سازمان‌ها و کاهش تهدیدات روزافزون سایبری توسعه یافته‌اند و همواره در مسیر ارتقا و به‌روزرسانی قرار دارند.

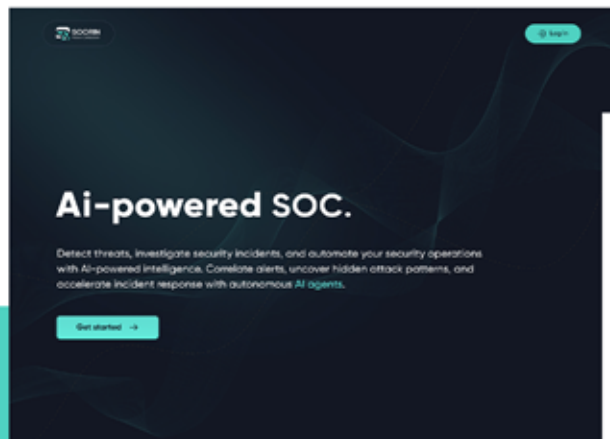
04

Alert Sharing

ابزار Alert Sharing یک سامانه پیشرفته برای جمع‌آوری، پردازش و اشتراک‌گذاری لاگ‌ها و هشدارهای امنیتی از منابع مختلف است که داده‌ها را در قالب‌های استاندارد مانند STIX و IODEF منتقل می‌کند.

از هشدار تا تصمیم آگاهانه

سامانه‌ای مبتنی بر هوش مصنوعی و عامل‌های هوشمند (AI Agents) که با خودکارسازی فرایند بررسی هشدارها، تحلیل شواهد و همبستگی رخدادهای امنیتی، به کارشناسان SOC در شناسایی تهدیدها و تصمیم‌گیری سریع‌تر و دقیق‌تر کمک می‌کند.



AI-Powered SOC

هوشمندسازی عملیات امنیت سایبری

جریان کاری هوشمند

دریافت هشدار

پردازش و همبستگی

تحلیل توسط Agentها

ارزیابی نتیجه

ایجاد پرونده امنیتی

پیشنهاد اقدام پاسخ‌گویی

قابلیت‌های کلیدی

• داشبورد مدیریتی

نمای کلی هشدارها، پرونده‌ها، وضعیت Agentها و سلامت سرویس‌ها

• مدیریت پرونده‌های امنیتی

تجمع هشدارهای مرتبط، مستندسازی شواهد و پیگیری رسیدگی

• تحلیل هوشمند هشدارها

بررسی هشدارها، جمع‌آوری شواهد و ارائه نتایج توضیح‌پذیر

• مدیریت Agentها

نمای کلی هشدارها، پرونده‌ها، وضعیت Agentها و سلامت سرویس‌ها

• مدیریت Playbookها

تعریف و پیگیری گردش کارهای پاسخ‌گویی و مراحل اجرای آن‌ها

• ردیابی و شفافیت

مشاهده تاریخچه تحلیل، دلایل تصمیم‌ها و وضعیت اقدامات پیشنهادی

ارزش عملیاتی برای تیم SOC

- کاهش زمان بررسی و ارزیابی هشدارهای امنیتی
- افزایش شفافیت در فرایند تحلیل و تصمیم‌گیری
- تسهیل پیگیری رخدادها و مدیریت پرونده‌های امنیتی
- حفظ کنترل انسانی بر اقدامات حساس و پاسخ‌گویی

پلتفرم آموزش و آگاهی رسانی سکتور

سکتور، پلتفرمی جهت تولید و عرضه محتوای آموزش تعاملی و آگاهی رسانی امنیتی است

دوره‌های تخصصی دفاع سایبری سورین عبارتند از:

- دوره اختصاصی و جامع مرکز عملیات امنیت
- دوره اختصاصی شناسایی تهدیدات سایبری
- دوره اختصاصی راهبری نرم افزارهای مطرح مانیتورینگ (Splunk، ELK، Wazuh) و ...)
- دوره اختصاصی پاسخگویی به حوادث سایبری (CSIRT)
- دوره‌های پایه امنیت سایبری (CEH، Security+ و ...)
- دوره‌های اختصاصی و سفارشی مطابق با نیازهای دانشی سازمان



رتبه بندی مخاطبان از نظر مهارت



آزمون و اعطای گواهی



ایجاد سریع آموزش تعاملی



لابراتور آنلاین جهت تمرین



یادگیری هدفمند و گام به گام



یادگیری باروشی سریع و به صرفه



- آموزش‌های تعاملی و گام به گام مورد نیاز خود را ایجاد کنید
- از آموزش‌های تعاملی و چند رسانه‌ای موجود بهره‌مند شوید
- از جدیدترین آسیب پذیری‌ها و هشدارهای امنیتی مطلع شوید
- در آزمون‌های تستی و عملیاتی شرکت کنید و مهارت خود را محک بزنید
- از یک محیط آزمایشگاهی آنلاین با سناریوهای از پیش تعریف شده بهره‌مند شوید



سازمان هواپیمایی
کل کشور



قوه قضائیه



شرکت توسعه
نیروگاه‌های حرارتی مینا 2



شرکت طراحی مهندسی
و تامین قطعات ایران
خودرو (ساپکو)



شرکت توانیر



موسسه مالی
و اعتبار ملل



آستان قدس رضوی

اعتماد سازمان‌های پیشرو به سورین

سازمان‌ها و شرکت‌های پیشرو در صنایع مختلف، برای مدیریت و هوشمندسازی دارایی‌های خود به سورین اعتماد کرده‌اند.



بانک قرض
الحسنه مهر



پتروشیمی پارس



سازمان بهزیستی
کل کشور



بانک سامان



فناواکارت



کارگزاری صبا جهاد



شرکت فولاد
مبارکه اصفهان



مرکز مبادله ارز
و طلای ایران



بانک مسکن



وزارت نیرو
جمهوری اسلامی ایران



بانک توسعه تعاون



بانک پارسیان



بانک سپه



بیمه دانا



بانک سینا

مجوزها و گواهی نامه ها

تعهد سورین به ارائه خدمات حرفه ای و منطبق با استانداردها، با دریافت مجوزها و تأییدیه های معتبر ملی و تخصصی



وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

- مجوز پیاده سازی مرکز عملیات امنیت و تیم پاسخ به رخداد از مرکز افتا
- مجوز امن سازی و مقاوم سازی سامانه ها و زیرساخت از مرکز افتا
- مجوز آموزش سازمان پدافند غیر عامل



شورای عالی انفورماتیک کشور

- مجوز آموزش از مرکز افتا
- مجوز آموزش از مرکز سمتا
- مجوز راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد از مرکز افتا

- مجوز دانش بنیان بر روی خدمات تولید و ارائه USECASE های امنیتی
- مجوز سازمان پدافند غیرعامل در حوزه مرکز عملیات امنیت
- رتبه یک شورای انفورماتیک در زمینه خدمات امنیتی



رئاست جمهوری
معاونت علمی، فناوری و اقتصاد دانش بنیان
معاونت توسعه شرکت های دانش بنیان



سازمان نظام صنفی رایانه ای کشور

- مجوز نظام صنفی رایانه ای کشور
- مجوز آموزش سازمان پدافند غیر عامل

تماس با ما

برای دریافت مشاوره، آشنایی با محصولات و خدمات سورین یا آغاز همکاری، کارشناسان ما آماده پاسخگویی به شما هستند.



SOORINSEC
Security

تلفن ثابت: ۰۲۱۲۲۰۲۱۷۳۴

تلفن همراه: ۰۹۰۲۸۹۹۰۵۵



تهران خیابان نلسون ماندلا، خیابان عاطفی غربی،
پلاک 85، طبقه پنجم واحد 9_10



www.Soorinsec.ir

